

-
2. (Amended) A computer-readable medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device, the method comprising:

A1

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and

making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the digital signature in a packet option.

5. (Amended) A computer-readable medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

A2

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data,

wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.

-
8. (Amended) A computer-readable medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device, the method comprising:

A3
hashing the public key;

comparing a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion;

if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing; and

if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing.

10. (Amended) A computer-readable medium containing instructions for performing a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device, the method comprising:

A4
hashing the public key and at least a portion of the route prefix of the network address;

setting the node-selectable portion of the network address to a portion of the value produced by the hashing;

checking to see if the network address as set is already in use; and

if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking.

17. (Amended) A computer-readable medium containing instructions for performing a method for a second computing device to maintain a cache of at least one public key/network address association, the method comprising:

AS
accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device; and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data.

20. (Amended) A computer-readable medium containing instructions for performing a method for a computing device to use a cache of at least one public key/network address association, the method comprising:

AL
accessing authentication information made available by a first computing device, the authentication information including content data, a public key of the first computing device, and a network address of the first computing device;

comparing the public key and network address of the first computing device with a public key/network address association in the cache; and

accepting the content data if the public key and network address of the first network device match the public key/network address association in the cache.

21. (Amended) A computer-readable medium having stored thereon a data structure of authentication information, the data structure comprising:

a first data field containing data representing a public key of a computing device; and

a second data field containing data representing a network address of the computing device, the network address derived, at least in part, from a hash of the public key.